

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Informatique et libertés

Poullet, Yves

Published in:
Entreprise et l'Homme

Publication date:
1981

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):
Poullet, Y 1981, 'Informatique et libertés', *Entreprise et l'Homme*, Numéro 2, p. 91-93.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Informatique et libertés

Yves POULLET,

Centre Informatique et Droit,
Facultés Universitaires de Namur.

Le développement des techniques informatiques appelle des slogans contradictoires : « L'informatique, découverte essentielle au devenir de l'humanité », « L'informatique, menace pour notre vie privée ».

Les pays⁽¹⁾ qui ont élaboré un « droit de l'informatique » ont tenté chacun à leur manière de trouver l'impossible compromis entre les deux thèses. Dans notre pays, le projet dit H. Vanderpoorten : « **Protection de certains aspects de la vie privée** » est indiscutablement marqué par la crainte du danger que représente pour la vie privée l'outil informatique.

Même si ce projet est aujourd'hui abandonné et si d'autres avant-projets sous les ministres Calewaert et Deworme ont vu le jour, il reste néanmoins un point de référence indiscutable pour notre gouvernement.

Il nous appartient dès lors de réfléchir à la valeur de la philosophie qui inspire le projet Vanderpoorten. Est-ce bien par le biais exclusif de la défense de la vie privée que peuvent et doivent être résolues les questions posées à nos sociétés par l'informatique ?

Ma réponse est négative. Le débat n'est pas celui « informatique (contre) vie privée » mais bien celui « informatique et libertés » selon le titre de la récente loi française. Ainsi, il est nécessaire de quitter l'approche « vie privée », approche essentiellement négative, et de lui préférer celle du « droit à l'information ».

La nécessité de ce passage a été profondément ressentie lors du colloque « **Banques de données - Entreprises - Vie Privée** » tenu à Namur les 25 et 26 septembre 1979⁽²⁾. Mes réflexions développeront dès lors ce que je crois être l'idée maîtresse de ce colloque.

1. La vie privée : une approche négative et dangereuse

Il est habituel de présenter l'individu comme étant agressé par l'informatique. Sa vie privée est en danger et l'informatique sociétaire devient un monstre pour l'individu en quête de « vie privée », c'est-à-dire d'anonymat.

Cette philosophie rousseauiste commande la mise en place d'un système lourd de règlements d'autorisation et de contrôle. Toute banque de données nominatives présente d'emblée un motif de crainte pour l'individu.

En outre, pour une série d'informations dites « données sensibles ou interdites » qui constituent le contenu minimal de notre vie privée (données médicales, judiciaires au sens large, opinions religieuses, politiques, syndicales, mutualistes, etc.), il faut interdire collecte et traitement.

Mécanisme lourd de règlements d'autorisation et de contrôle, liste longue de données « interdites », voilà, en bref, la structure du projet Vanderpoorten dictée, dit-on, par les abus de l'informatique.

Je ne blanchis pas l'informatique de ces accusations mais prétends que ce n'est pas par le biais du slogan « vie privée » qu'une loi pourra remédier sérieusement à de tels abus.

J'ai toujours été étonné de l'effort stérile des doctrinaires français à trouver une définition quelque peu précise de la vie privée. A cet égard, je préfère la solution pragmatique adoptée par les Anglais : elle refuse toute définition du concept et se contente de pouvoir affirmer que dans tel cas d'espèce — in concreto — il y a atteinte à cette zone d'intimité qu'est la vie privée.

Car, sans vouloir aller jusqu'aux affirmations du juriste et sociologue italien Stefano Rodotà pour qui la vie privée est née avec la civilisation bourgeoise et urbaine (que pourrait en effet signifier la « vie privée » dans certains de nos villages ?), il faut cependant admettre que la vie privée n'est pas un concept aux contours clos mais un éternel relatif. Il n'y a pas de vie privée en soi mais toujours relativement à un « pour qui » et un « pour quoi faire ». Ainsi, appliquant cette affirmation aux données dites « sensibles » ou « interdites », présentées comme le noyau dur de la vie privée, nul ne contestera que la donnée sur le passé judiciaire « escroquerie » ou « chèque sans provision » puisse figurer, du moins pendant un certain temps, dans la banque de données tenue par la société bancaire où le client failli ou émetteur de chèque non provisionné a son compte.

De même, rien ne peut être moins privé que les convictions religieuses, politiques ou syndicales d'un militant et votre race ne peut être cachée au simple passant. Qu'on ne nous parle pas de vie privée à ces propos..., qu'on nous dise — et ce sera plus juste — que l'énoncé abstrait de telles informations peut être source de discriminations pour le fiché et qu'il n'est bon dès lors de permettre leur enregistrement que dans les cas où la reprise de cette donnée est absolument nécessaire à l'accomplissement des fins légitimes — contractuelles ou réglementaires — de l'endroit collecteur. C'est un problème de discrimination et non de vie privée.

Aussi, il est absurde de prétendre défendre ou réglementer a priori le traitement de telle

⁽¹⁾ La liste des principaux projets et lois nationaux est reprise en annexe de l'article.

⁽²⁾ Les références sont dans la bibliographie en annexe de l'article.

ou telle information. Cette solution oblige à multiplier les exceptions chaque fois que le traitement de la donnée sera, in casu, à considérer comme « pertinent », « adéquat » à la finalité de la banque de données.

Il y a donc lieu de substituer à l'approche analytique de l'information, approche que suppose l'illusion d'une définition de la vie privée, celle fonctionnelle : une information n'est pas dangereuse « en soi » mais bien par sa place dans un tout finalisé.

C'est cette fin poursuivie par le traitement qui, seule, peut justifier le « droit à l'information » du collecteur, et c'est seulement au regard des nécessités de cette fin que doit être jugée la « pertinence » de la donnée recueillie.

Fondamentalement, notre protestation en faveur de la vie privée cache en effet une contestation bien plus importante, celle du « droit à l'information » des collecteurs.

Monsieur Pardon, lors de notre colloque, exprimait la même idée par cet exemple : l'administration des contributions communales par ordinateur, des renseignements fiscaux à des organismes de sécurité sociale et ce, à l'insu de l'intéressé, c'est-à-dire sans que ce dernier puisse redresser les éventuelles erreurs. Cette communication est par ailleurs prévue légalement. Irons-nous dire que l'ordinateur a une fois de plus agressé notre vie privée ?

Le problème n'est décidément pas là. La seule question qu'il convient de poser est celle de la correspondance entre la loi votée et la société démocratique voulue. Si cette correspondance existe, alors l'ordinateur ne fait que rendre efficace le « droit à l'information » légitime de l'organisme de sécurité sociale.

En d'autres termes, l'équilibre entre, d'une part, les exigences d'information des collecteurs et, d'autre part, le respect de nos libertés nécessite pour sa solution un débat démocratique où la question du choix de société est clairement posée. L'ordinateur n'est, en définitive, que le révélateur de cette exigence.

La solution toujours relative du débat « Informatique et libertés » exige donc, on le pressent, que l'on double le « droit à l'information » des collecteurs, d'un véritable « droit à l'information » des « fichés ». Ce n'est que dans la mesure où ces derniers peuvent connaître et, par des mécanismes démocratiques, contrôler le droit à l'informa-

tion des collecteurs, que peut être défini clairement un type de « vouloir vivre social ».

C'est l'équilibre de ces deux « droits à l'information » que je vais tenter de décrire sous l'angle particulier des entreprises.

2. Le droit à l'information

A. Le droit à l'information des collecteurs, en particulier des entreprises

Monsieur Lebrun, dans un remarquable exposé au colloque, affirmait que l'Etat fondait son droit à l'information sur ses prérogatives de puissance publique soumises dans une société démocratique parlementaire aux principes de légalité, de proportionnalité et de spécialité.

Ceci impliquerait notamment que toute décision relative à l'outil informatique de l'administration devait être contrôlée directement ou indirectement par le parlement.

Parallèlement, c'est dans la relation contractuelle libre avec le fiché que la plupart des entreprises puisent leur droit à l'information. Le critère de « pertinence » déjà affirmé par la résolution 73(22) du Conseil de l'Europe et explicité par la loi allemande de 1977 doit alors servir de guide dans l'appréciation des limites du droit à l'information de l'entreprise collective : « Le traitement, le stockage ou l'utilisation de l'information est-il bien nécessaire à la bonne fin du service contractuel attendu ? » Ce principe appelle à la fois certaines conséquences et certaines limites.

Parlons d'abord des limites : le critère de « pertinence » en relation avec la liberté contractuelle doit avoir pour toutes les entreprises non « monopolistiques » qu'elles appartiennent aux secteurs privé ou public dans la mesure où ces entreprises travaillent directement dans le cadre de leur relation contractuelle avec le fiché. Nous excluons dès lors :

- 1°) toute entreprise monopolistique, entreprise où la liberté contractuelle ne peut exister ;
- 2°) tout traitement, même effectué par une entreprise en situation de concurrence, qui ne découlerait pas directement de la relation contractuelle avec le fiché (fichier « marketing », par exemple) ;
- 3°) toute entreprise, enfin, ne travaillant pas en relation contractuelle, tels les éditeurs d'adresses et les agences de renseignements commerciaux pour lesquels des

règles spéciales sont prévues dans de nombreuses législations étrangères.

Les conséquences du principe sont de trois ordres :

1) l'enregistrement et le traitement des données par une entreprise travaillant dans le cadre de sa relation contractuelle avec le client fiché sont libres puisque fondés sur la liberté contractuelle. Il n'est donc pas nécessaire de prévoir l'autorisation préalable pour les banques de données des entreprises citées.

Cette remarque n'exclut en aucune façon un contrôle a posteriori par un organisme ad hoc, sorte d'Ombudsman représentant les intérêts des fichés, mais c'est en dernier ressort au juge du judiciaire d'apprécier, en fonction du contexte social d'une époque, c'est-à-dire de façon souple, quelles données se révèlent nécessaires pour l'accomplissement du but poursuivi par le contrat auquel le fiché a adhéré librement.

2) le critère de pertinence vaut tant pour le traitement des données individuelles que pour celui des données de l'entreprise (chiffre d'affaires, liste des fournisseurs, prix de revient, etc.). Cette conséquence permet d'éviter à notre avis le faux débat : « existe-t-il une vie privée des personnes morales ? ».

3) si le traitement interne d'une donnée, c'est-à-dire son utilisation au sein d'une entreprise découle incontestablement de la relation de l'entreprise avec le fiché, la communication de cette même donnée par l'entreprise collectrice à une autre entreprise doit faire l'objet d'un contrôle plus sévère.

D'une part, la communication ne peut être valable que si elle est conforme au but contractuel de la première entreprise, mais, qu'en outre, il peut être prouvé que la seconde entreprise a besoin des données transmises et qu'aucun préjudice n'en résultera pour le fiché.

L'exemple type est celui de la banque qui finance un achat à tempérament et désire assurer les risques liés à ce financement auprès d'une compagnie d'assurance-crédit. La communication de certaines données devra répondre aux critères énoncés.

B. Le droit à l'information du fiché

L'affirmation du droit à l'information du collecteur appelle comme corollaire le droit à l'information du fiché.

Différents aspects de ce droit à l'information doivent être soulignés.

Pour le public, en général, le droit à l'information consistera en un droit à l'enseignement de ce qu'est l'informatique et de ses potentialités d'action. Il s'agit de démystifier l'outil informatique afin de pouvoir apprécier à leur juste valeur les mérites et les dangers de l'ordinateur (cfr à cet égard, la récente décision gouvernementale française à propos de l'ordinateur dans l'enseignement).

Cela ne suffit certes pas, il est nécessaire que le public puisse aussi disposer d'une série d'informations — et on pense ici à la création d'un registre public — sur chaque centre d'information (localisation, responsable, données utilisées, but de l'utilisation de ces données, caractéristiques techniques du système utilisé, utilisateurs internes et externes, etc.). Ce registre public permettrait d'assurer une certaine transparence des flux d'information et de leurs pouvoirs effectifs, et devrait être à la base du dialogue démocratique qui me paraît devoir s'instaurer entre fiché et collecteur.

En outre, pour le fiché, ce droit appelle une certaine maîtrise de l'image de lui-même telle qu'elle est exploitée par la banque de données.

Le droit à l'information signifie donc pour chaque fiché la reconnaissance d'un certain «droit à l'image». Ce droit doit s'entendre comme :

1) le droit de savoir où son image est utilisée et pourquoi elle est utilisée. Si le fiché connaît naturellement l'utilisation de son image par les entreprises travaillant dans le cadre de la relation contractuelle, il est peut-être nécessaire de prévoir qu'il soit averti dans les autres cas. C'est-à-dire chaque fois qu'une entreprise ne travaille pas dans le cadre d'une ou de la relation contractuelle et chaque fois qu'il y a communs des données.

2) le droit d'exiger que l'image utilisée soit conforme à la vérité (affectation de la donnée d'un certain indice de doute) ou complétée. Ce droit doit, à mon avis, s'exercer d'abord auprès du collecteur. Il serait peut-être utile de prévoir en outre des procédures judiciaires rapides pour de telles vérifications.

3) le droit de contester l'utilisation de son image. Ce dernier point m'apparaît le plus important. Il s'agit pour le fiché, de préciser

et limiter l'étendue du «droit à l'information» du collecteur, en affirmant la non-pertinence d'une donnée et le risque de discrimination que son utilisation dès lors entraîne. Il y a donc, dans ces hypothèses, conflit de droits. S'il est bien évident que la décision doit être prise par le juge naturel, même si le droit à l'information du fiché exige la mise en place d'organes capables de définir le juste équilibre toujours relatif entre les deux droits en cause, le droit à l'information du fiché doit permettre la mise en place préventive de mécanismes démocratiques de contrôle du droit à l'information des collecteurs : une sorte d'Ombudsman, d'office de contrôle.

Cet office ne peut être un lobby de technologues. Il représente les intérêts des fichés et a pour tâche d'alerter les pouvoirs constitutionnellement désignés pour trancher.

Que le juge — et c'est ainsi que je conclus — puisse par lui comprendre que l'informatique ou plutôt l'information est un outil de pouvoir et qu'il importe dès lors de contrôler les moyens de ce pouvoir. Ou à la question : «Où s'arrête le «droit à l'information» des entreprises et des administrations?», il est absurde de répondre... «à la vie privée des citoyens». Vous cherchiez en vain une quelconque signification à ce slogan. Qu'au contraire, cet office rende chaque citoyen, chaque fiché, conscient qu'au-delà de sa propre protestation individuelle, il aide à la définition de ce que Jacques Berleur, lors du colloque, appelait un «type de vouloir vivre social».

Voilà en effet, le véritable problème que l'informatique révèle plus qu'elle ne pose.

□

Liste de quelques textes de loi

- Autriche : Datenschutzgesetz, 18 octobre 1978
- Conseil de l'Europe : Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 21 janvier 1981
- Danemark : Loi danoise n° 293 sur les registres privés, 8 juin 1978. Loi danoise n° 294 sur les registres publics, 8 juin 1978
- France : Loi n° 78-17 du 6 janvier 1978 : Informatique, Fichiers et Libertés
- Luxembourg : Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques
- Norvège : Loi du 9 juin 1978 sur les registres de personnes
- République Fédérale Allemande : Bundesdatenschutzgesetz, 27 janvier 1977
- Suède : Data Act du 11 mai 1973 (amendé le 1 juillet 1979) et Fair Credit Reporting Act 1973
- USA : Privacy Act 31 décembre 1974 - Fair Credit Reporting Act 1970.

Pour la Belgique

Le projet dit «Vanderpoorten» «relatif à la protection de certains aspects de la vie privée», Doc. Parl. Sénat, 1975-1976, n° 846, 8 avril 1976, 1. Non relevé de caducité par le dernier gouvernement.

Bibliographie sommaire

- Banques de données - Entreprises et Vie Privée, Actes du colloque des 25 et 26 septembre 1979, Bruxelles, CREADIF, 1980. (Présenté dans L'Entreprise et l'Homme, 1981, 1, page 59).
- Berleur J. et Pouillet Y., Informatique et Vie Privée, Enjeux réels, Interdoc, Périodique, septembre 1978, 6 et s.
- Turn R., Privacy Protection in Record keeping Systems, Inf and Management, Périodique, 1978, 187-197.
- Aronstein C.S., De l'urgence d'ordonner les ordinateurs, Journal des Tribunaux, 1980.
- Questions d'ordre politique soulevées par la protection des données des libertés individuelles, Paris, OCDE, Etudes Informatiques, 1976, n° 10.